# July 2002 Upgrade Change Details

During the month of July 2002, **newly upgraded Cryptocard servers** went go into production

This upgrade included:

1. New hardware.
2. Changes to the database used by the original servers.
3. Improvements in synchronization between servers, and between server and user.
4. Changes to the ST-1 software tokens and PT-1 Palm Pilot tokens.
5. Support for Windows ME software tokens and Mac OS 9/X software tokens.

# Synchronization Improvements

There are three conditions that can exist re: synchronization: 1) your token's challenge/response is exactly in sync with the server, 2) your token's challenge/response is "ahead" of the server, 3) the server's challenge/response is "ahead" of your token.

*On the original server (up until July 2002):* The original server anticipated your next 'n' responses (usually n=10) to its challenges, allowing for your token to be "ahead" of the server but still successfully authenticate... that was good! But what happened if, at another time, you were perfectly in sync with the server, but you happened to mistype your password response one time... the server moved on and offered up the NEXT challenge which you may not have seen, so you tried the same password response again... that was bad!... the server was now "ahead" of your token... it offered up a new challenge and you were still trying to type in the previous response... you were now out-of-sync with the server! This is why we have always suggested you advance your token thru a few (3 or 4) challenge/response cycles if you were failing authentication, so you could get back in sync.

*On the upgraded server (after July 2002):* The upgraded server still anticipates your next 'n' responses, so your token can still be "ahead" of the server and result in successful authentication. Additionally, the upgraded server refrains to some degree from advancing ahead of your token when you have simply mistyped your password response a few times, or even when you have inadvertently hit a carriage return and effectively entered nothing for a password response. It does this by allowing you to make a certain number of attempts to type in the current password response... this is good! What it means is that the server won't automatically jump "ahead" of your token when you make a few mistakes at the keyboard, so if you were in sync to begin with, you'll stay in sync until you get it right. (There is, of course, a cap on the number of attempts you are allowed; otherwise, its assumed someone is trying to break in with your username, and

your account will be disabled.) It also means that there are fewer chances of your token getting out of sync with the server. So, if you are failing authentication repeatedly, you can safely assume its because you're out-of-sync... in most instances you can simply advance your token a few (3 or 4) challenge/response cycles to get back in sync; if that fails, you'll still be able to resync your token via the usual methods described in the Cryptocard Token User Guide.

Also on the upgraded servers, synchronization between the primary and secondary Cryptocard servers has improved. In the past if there were a server failure or a network failure on the primary server and you failed over to the secondary server, often the servers were not closely enough synchronized such that you would have to resync your token before using it again; a change in the database used on the upgraded servers allows for close synchronization between the primary and secondary server. The ultimate goal of Cryptocard is to make synchronization a NON-issue to its users.

## Changes to ST-1s (software tokens) and PT-1s (Palm Pilot tokens)

Due to the synchronization improvements above and Cryptocard's goal of minimizing concerns about synchronization, they have made some changes to the software versions of their tokens.... specifically, the ST-1 and the PT-1 tokens. Cryptocard has plans to incorporate the software version of their tokens in other product lines in the future and so are moving towards simplifying the tokens. ST-1s and PT-1 tokens distributed prior to July 2002 will continue to work with the upgraded Cryptocard servers. HOWEVER, if for some reason you need to acquire a new token configuration file (<username>.tok for ST-1s; <username>.pdb for PT-1s) from the Account Management Office, you will first have to upgrade your ST-1 or PT-1 application to the latest version available.

Users may voluntarily upgrade their current ST-1s or PT-1s to the newest version if they wish. Doing so would require you to obtain the newest ST-1 or PT-1 application file from the appropriate web page, and then request that the Account Management Office reinitialize your ST-1 or PT-1 and send you a new .tok file or .pdb file.

Although the upgraded PT-1 token has not changed much visually, the upgraded ST-1 has changed considerably. The original ST-1 had two options for a display interface with the user... a standard GUI (Graphical User Interface) which popped up a window prompting you for a PIN# and displayed to you your challenge and response; or an RB-1 Emulation Interface that attempted to emulate the RB-1 hardware token with a calculator type keyboard interface. The RB-1 emulation interface is removed in the upgraded ST-1s, and the remaining GUI interface no longer shows a challenge to the user, but instead only shows a response. With the synchronization improvements introduced in the upgraded server, users should have an easier time staying in sync with the server; with this in mind, the challenge was removed from the GUI display. Of course, as always,

users can still input the current server challenge into the upgraded ST-1 if they need to resync their tokens.

## Additional new ST-1 software tokens available

In addition to the ST-1 software token application which can be loaded on Windows 2000/NT/98/95, Linux, and Unix (Solaris), the upgraded servers also support ST-1s on Windows ME and Mac OS 9/X. Although ST-1s are not officially supported on XP, they are likely to work on that platform as well. As always, ST-1s are likely to run on any platform which can support the Java™ RunTime Environment (JRE) 1.1.7+, but they are not officially supported for anything other than the platforms specifically mentioned in this paragraph (excluding XP).

## Got Questions or Need Help

As always, users can **contact the ITD Service Desk at x5522** if they are experiencing any problems. Opening up a Service Desk ticket will ensure your inquiries are dealt with most effectively.